

CLAIMS

What is claimed is:

1. A proxy process for emulating card-present credit card transactions in credit card purchase transactions occurring remotely between a credit cardholder's computer and a merchant server over a computer network, the process comprising:
 - (a) collecting credit card information and identification information at a designated identifier;
 - (b) transmitting the collected credit card information to an authentication server connected to a computer network;
 - 10 (c) performing an identification transaction wherein the authentication server determines whether the cardholder is authorized to use the credit card and, if so, the authentication server issues a code temporarily binding the identity of an individual possessing the code, the credit card information and the identification information to that of the credit cardholder who presented the credit card to the identifier;
 - 15 (d) creating a record of the identification transaction including the credit card information, the code, and the identity of the credit cardholder on the authentication server sending the code to the identifier and cardholder;
 - (e) entering the credit card information and the code into the cardholder's computer and sending the credit card information and code from the cardholder's computer to the authentication server over a computer network;
 - 20 (f) comparing on the authentication server the credit card information and code submitted from the cardholder's computer to the credit card information and code stored in the record of the identification transaction ;

(g) completing the identification transaction by transmitting a digital certificate from the authentication server to the cardholder's computer when the card information and the code submitted from the cardholder's computer match the card information and code stored in the record of the identification transaction on the authentication server;

(h) the cardholder entering a purchase transaction with a merchant over a computer network from the cardholder's computer to the merchant server by offering the credit card information and digital certificate as payment; and

(i) the merchant web server validating the digital certificate from the authentication web server before authorizing the credit card purchase transaction.

2. The proxy process of claim 1 wherein the designated identifier comprises an automated teller machine and the step of performing an identification transaction comprises:

(a) the credit cardholder presenting the credit card to the automated teller machine such that the automated teller machine reads magnetically coded data stored on a magnetic stripe formed on the credit card; and

(b) the automated teller machine verifying that the personal identification number entered by the credit cardholder matches a personal identification number previously assigned to the credit card.

3. The proxy process of claim 1 wherein the designated identifier is a human agent having access to a credit card point-of-sale terminal and wherein the step of performing an identification transaction comprises:

- (a) swiping the credit card through the point-of-sale terminal to read data magnetically encoded on a magnetic stripe on the credit card;
- (b) generating a paper receipt to record the transaction;
- (c) the credit cardholder signing the receipt; and
- (d) the agent comparing the signature on the receipt to a signature signed on the credit card.

4. The proxy process of claim 3 wherein the step of performing an identification transaction further comprises determining whether the personal identification number entered by the cardholder matches a personal identification number previously assigned to the card.

5. The proxy process of claim 1 wherein the designated identifier is a human agent having access to a credit card point-of-sale terminal and wherein the step of performing an identification transaction comprises;

- (a) swiping the credit card through the point-of-sale terminal to read data magnetically encoded on a magnetic stripe on the credit card; and
- (b) the agent viewing a picture identification of the cardholder.

6. The proxy process of claim 1 wherein the step of performing an identification transaction further comprises transmitting to the authentication server the biometric data collected as part of the identification information, and storing the biometric data with the record of the proxy transaction.

5

7. The proxy process of claim 6 wherein the authentication server contacts a web server of the credit cardholder's card issuer and compares the data received from the cardholder with cardholder data previously received by the card issuer's web server.

10

8. The proxy process of claim 7 further comprising the steps of:

(a) the cardholder transmitting biometric data associated with the cardholder to the merchant; and

(b) verifying whether the biometric data transmitted by the cardholder to the merchant matches the biometric data obtained during the identification transaction.

15

9. The proxy process of claim 8 wherein the step of obtaining biometric data comprises obtaining a digital finger print of the cardholder.

20

10. The proxy process of claim 8 wherein the step of obtaining biometric data comprises obtaining a retinal scan of the cardholder.

11. A secure payment method whereby a merchant accepting a credit card as payment from a customer over a computer network may be reasonably assured that the

customer tendering the credit card is a person authorized to use the card, the method comprising the steps of:

- 5 (a) performing a proxy card-present transaction where the customer's identity is positively established by submitting the customer's credit card information and biometric information to an identification agent;
- (b) providing a unique code to the customer whereby it may be presumed that a person possessing information from the face of the credit card and the unique code is the person who presented the credit card during the proxy transaction;
- 10 (c) storing a record of the proxy transaction on a database stored in an authentication server;
- (d) contacting the authentication server from the customer's computer over the network and submitting the unique code and the customer's credit card information to the authentication server for comparison with the record of the proxy transaction stored in an authentication server database;
- 15 (e) comparing the credit card information and the unique code and, if they match, issuing a secure pay digital certificate to the customer and storing the secure pay digital certificate on the customer's computer;
- (f) the customer entering transaction data with the merchant over the network and tendering the credit card as payment; and
- 20 (g) the merchant checking for the presence of the secure pay digital certificate on the customer's computer and, upon finding the secure pay certificate, verifying that the certificate and the credit card information tendered by the customer are valid.

12. The secure payment method of claim 11 wherein the step of performing a proxy card-present transaction comprises the customer presenting the credit card to an identification agent, the identification agent reading electromagnetically coded data from the card and positively identifying the customer.

13. The secure payment method of claim 12 wherein the step of performing a proxy card-present transaction further comprises the identification agent recording biometric data from the customer.

14. The secure payment method of claim 13 further comprising the step of the customer submitting biometric data to the merchant along with the credit card information when the credit card is tendered as payment, and wherein the step of verifying that the certificate and the credit card information are valid includes the step of comparing the biometric data submitted by the customer to the biometric data collected by the identification agent.

15. The secure payment method of claim 14 wherein the step of recording biometric data comprises recording a digital finger print.

16. The secure payment method of claim 14 wherein the step of recording biometric data comprises recording a retinal scan.

17. The secure payment method of claim 14 wherein the identification agent comprises an automated teller machine.

18. The secure payment method of claim 14 wherein the identification agent
5 comprises a human attendant having a credit card point-of-sale terminal.

19. The secure payment method of claim 11 wherein the step of issuing a computer readable certificate comprises encoding a PKI digital certificate onto a portable token removably connectable to a computer port.

10

20. The secure payment method of claim 11 wherein the step of issuing a computer readable certificate comprises transmitting a PKI encoded digital certificate to the customer's computer over a computer network.

15

21. The secure payment method of claim 11 wherein the database operates in conjunction with an authentication web server and the step of the merchant verifying the validity of the certificate on the customer's computer comprises redirecting the transaction to the authentication web server over a computer network, and the authentication server determining whether the certificate and the credit card information

20

submitted by the customer are valid.

22. The secure payment method of claim 11 wherein the step of the merchant checking for the presence of the secure pay digital certificate on the customer's

computer comprises: the merchant initiating a PKI session by checking the customer's browser and, if the secure pay certificate is located therein, the merchant retrieving the certificate information and sending it to the authentication server to verify that the certificate is still valid.

5

23. The secure payment method of claim 11 and the step of monitoring credit card usage transactions for fraudulent activity.

24. The secure payment method of claim 11 wherein after the merchant verifies the
10 validity of the secure pay digital certificate and credit card information tendered by the customer, transmitting the customer's credit card information from the authentication server to the merchant.

25. The secure pay method of claim 11 wherein after the merchant verifies the
15 validity of the secure pay digital certificate and credit card information tendered by the customer, transmitting the customer's biometric information from the authentication server to the merchant.

26. The secure payment method of claim 11 wherein step (d) includes creating a
20 record of biometric information in the authentication server database.

27. A system for providing a proxy card-present transaction for a credit card transaction occurring over a computer network, whereby a merchant receiving payment

via the credit card over a computer network may be reasonably assured that a customer tendering the credit card is an individual authorized to use the credit card, the system comprising:

- (a) an identity verification agent, a customer computer, a merchant server,
5 and an authentication server, all being interconnected over a computer network;
- (b) the identity verification agent including means for positively identifying the customer when the customer personally presents the credit card to the identity verification agent, and means for transmitting a record of the positive identification along with information from the credit card to the authentication server;
- 10 (c) the authentication web server configured to generate a unique code associated with the positive identification, store the record of the positive identification along with the code, and transmit the code to the identity verification agent for presentation to the customer;
- (d) the customer computer including input means for receiving information
15 from the credit card along with the code generated by the authentication server and output means for transmitting the code and credit card information to the authentication server;
- (e) the authentication server further including means for comparing the credit card information and code received from the customer computer with that
20 previously stored on the authentication server as a result of the positive identification by the identity verification agent, means for generating a unique digital certificate, and means for transmitting the certificate to customer computer; and

(f) the merchant server including means for determining whether a valid digital certificate issued from the authentication server is present on the customer computer.

5 28. The system of claim 27 wherein the identity verification agent comprises an automated teller machine interconnected with an automated teller machine network.

29. The system of claim 28 wherein the means for positively identifying the customer comprises an automated teller machine input device whereby the customer
10 may input a personal identification number, and means for determining whether the personal identification number entered by the customer is a correct personal identification number previously associated with the credit card.

30. The system of claim 27 wherein the identity verification agent comprises a
15 human attendant having a credit card point-of-sale terminal.

31. The system of claim 30 wherein the means for positively identifying the customer comprises the attendant viewing a picture identification of the customer.

20 32. The system of claim 30 wherein the means for positively identifying the customer comprises the attendant comparing a customer signature made in the attendant's presence with a customer signature on the credit card.

33. The system of claim 30 wherein the means for positively identifying the customer comprises a personal identification number entered by the customer into the point-of-sale terminal, the point of sale terminal verifying whether the number entered by the customer is correct via a point-of-sale terminal network.

5

34. The system of claim 27 further including means for the identity verification agent to record biometric data from the customer when the identity verification agent positively identifies the customer.

10 35. The system of claim 34 further including means associated with the customer's computer for recording the customer's biometric data and transmitting the biometric data to the merchant web server.

15 36. The system of claim 35 further including means for comparing the biometric data recorded by the identity verification agent with that transmitted by the customer to the merchant.

37. The system of claim 36 wherein the biometric data comprises a digitized finger print.

20

38. The system of claim 36 wherein the biometric data comprises a retinal scan.



39. The system of claim 27 wherein the merchant web server means for determining whether a valid digital certificate is present on the customer's computer comprises: means for sending the certificate and the customer's credit card information from the merchant to the authentication server, whereby the authentication server determines
5 whether the certificate and the credit card information submitted by the customer are valid.

40. The system of claim 27 whereby the authentication server is operated by an agent of the merchant, and whereby authorization for the transaction is obtained by a
10 card issuer responsible for issuing the customer's credit card or a card issuer authorizing agent.

41. A process for increasing security in credit card transactions occurring remotely between a credit cardholder's computer and a merchant server over a computer
15 network, the process comprising:

- (a) reading a credit card containing information at a designated identifier;
- (b) performing an identification transaction wherein the identifier determines whether the cardholder is authorized to use the credit card and, if so, an authentication server issues a code temporarily binding the identity of an individual possessing both
20 the code and information printed on the credit card to that of the credit cardholder who presented the credit card to the identifier;



(c) creating a record of the identification transaction including the credit card information, the code, and the identity of the credit cardholder on an authentication server connected to a computer network;

(d) submitting the credit card information and the code from the cardholder's
5 computer to the authentication server over a computer network;

(e) comparing the credit card information and code submitted from the cardholder's computer to the credit card information and code stored in the record of the identification transaction on the authentication server;

(f) transmitting a digital certificate from the authentication server to the
10 cardholder's computer when the card information and the code submitted from the cardholder's computer match the card information and code stored in the record of the identification transaction on the authentication server;

whereby the presence of a digital certificate on the cardholder's computer indicates to the merchant's server in subsequent transactions with the cardholder's
15 computer that the cardholder is the owner of the card.